UCRL-JC-122612 Abs

Position Paper: Computer Security Technology Center

Lawrence Livermore National Laboratory
Contact: spcooper@llnl.gov

The **Computer Security Technology Center** (CSTC) was formed in the wake of the Internet Worm incident in 1988. It served as a focal point for the ongoing computer security research and development at the **Lawrence Livermore National Laboratory** (LLNL). It has evolved to three functional components: incident response, product development, and consulting services. The **Computer Incident Advisory Capability** (CIAC) took on the computer security incident response for the **Department of Energy** (DOE). The CSTC started research and development of the Security Profile Inspector (SPI) and Network Intrusion Detector (NID) packages. They are currently in use at a number of DOE and DOD sites. **Secure Systems Services** (S^3) was started in 1994 to provide information security consulting and professional services including security analysis and design, penetration testing, and other customized services leading to site-specific solutions.

Together, the three areas of the CSTC complement each other for the advancement of information security technology: CIAC provides current vulnerability and threat information; S^3 provides user requirements and constraints and creates real solutions; and the product development group researches leading-edge security issues and develops tools and methodologies to enhance the security posture of today's and tomorrow's computer systems and networks.

We envision the growing need for security components to effectively work together. The complexity and interplay of today's computers and networks make effective security management extremely difficult. Furthermore, the DOE is not immune from the downsizing that is so popular today. Therefore, these networks are increasingly being managed by fewer people. One approach is to have a centrally managed security policy database for a network. This would communicate with or be utilized by the various security tools such as firewalls, intrusion detection systems, host-based inspection tools, etc. In a joint project with Sandia National Laboratories, U.C. Davis, and Sun Microsystems, we have developed such a proposal for an advanced firewall system. This system would be able to adjust its security stance dynamically in response to threats. For example, it could adjust its auditing or shut down certain connections when it detected intrusion activity.

Two DOE initiatives or programs, the Accelerated Strategic Computing Initiative (ASCI) and the Advanced Design and Production Technologies (ADaPT) program, will also push the edge of information security technology. ASCI is looking at using security features in the Distributed Computing Environment (DCE) and ADaPT is looking at the Common Object Request Broker Architecture (CORBA) for application development. DCE is somewhat difficult to manage, and CORBA has limited to no security infrastructure. There will be a lot of work required in developing robust and manageable security for the applications using these technologies.

In the classified areas of the above initiatives, "need-to-know" will be a complex problem. This may push the access control requirements to the object, file, or even field level. It would be desirable to provide the access management capabilities directly to the owners of the data rather than a system manager.

These are areas we see with a high priority for information security research in the DOE. We are looking at organizations that face similar problems. One large example is the Department of Defense TransTech initiative which seeks to link together the military logistics and supplier community. However, that is a much more hierarchical, client-server model than the peer-to-peer, collaborative model required of the laboratory environments of the DOE.

This work was performed under the auspices of the U.S. Dept. of Energy at LLNL under contract no. W-7405-Eng-48.